

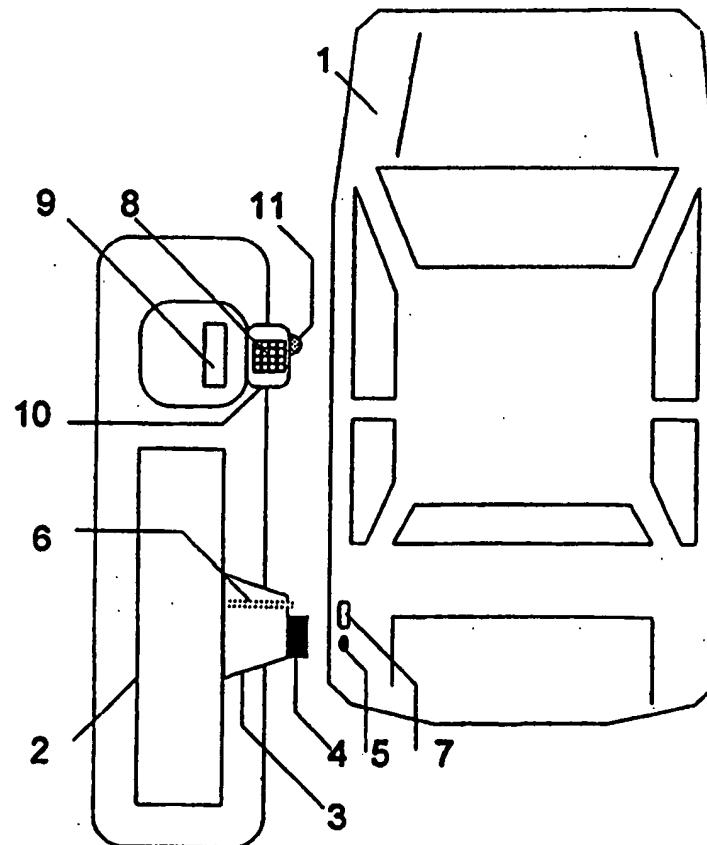


(51) International Patent Classification 6 :  B67D 5/08		A1	(11) International Publication Number: WO 95/32919
(21) International Application Number: PCT/SE94/00508		(81) Designated States: BR, CN, JP, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 27 May 1994 (27.05.94)			
(71)(72) Applicant and Inventor: GUNNARSSON, Staffan [SE/SE]; Svärdslijevägen 62, S-165 77 Hässelby (SE).		Published <i>With international search report. In English translation (filed in Swedish).</i>	
(74) Agents: ÖRTENBLAD, Bertil et al.; Noréns Patentbyrå AB, P.O. Box 27034, S-102 51 Stockholm (SE).			

(54) Title: SYSTEM AT A VEHICLE FOR DEBITING AT AUTOMATIC FUELING

**(57) Abstract**

System at a vehicle for automatic fuelling and debiting in relation to this, where a on the vehicle assembled transponder is used as well for the positioning of the fuelling robot as for the debiting function.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

## SYSTEM AT A VEHICLE FOR DEBITING AT AUTOMATIC FUELLING

The present invention relates to a system at a vehicle for debiting at automatic fuelling, where the driver does not have  
5 to leave the vehicle for paying the filled fuel.

## Background and aim of the invention

Automatic fuelling of vehicles is known among others from the  
10 Swedish patents 8403564-1 and 9002493-6, that show solutions where the position of the filling place is automatically measured by means of microwave technology, in that a fuelling robot senses the position of a position giving transponder assembled for the purpose close to the filling point of the  
15 vehicle. In this way a comfortable, safe and fast filling of fuel is obtained, without the driver having to step out of the vehicle.

Since usually a payment/debiting is related to the filling of  
20 fuel, it is also desirable to find solutions allowing that the payment operation itself does not require leaving the vehicle, since otherwise a big part of the advantages with automatic fuelling would be lost.

25 Hereby information about account, fuel quality etc can be stored in a transponder on the vehicle, for example in the transponder unit that is used for measuring of the position. Thereby the cost for a special data carrier and reader for the debiting is avoided, since common system components are used  
30 for the position measurement as well as for the debiting.

An aim with the present invention is to enable automatic debiting during automatic fuelling of vehicles without the driver in relation to this having to step out of the vehicle,  
35 and where the total cost of the system has been minimized.

A second aim with the invention is to solve the theft demand

problems for a transponder on a vehicle that may occur in case of using debiting functions in the transponder.

A third aim of the invention is to provide a solution that 5 allows an accurate measurement of the position of the transponder as well as that the transponder is communicated with data.

A fourth aim of the invention is to enable an off line 10 function, i e that the system shall not have to call a central to match the data code of the transponder with a personal code related to the driver of the vehicle and/or the fuelling place.

A fifth aim of the invention is to enable also the debiting in 15 itself off line, i e without having to call a central.

A sixth aim of the invention is to enable updating and reading 20 of the transponder both at the fuelling robot and at other places in a way which is acceptable from a security point of view.

#### Description of the invention

The present invention thus relates to a system for debiting at 25 automatic fuelling of vehicles, where a microwave transponder close to the filling point of the vehicle is used for positioning of a fuelling robot by position measurement with a sensor in the moving arm of the robot, and is characterized in that the transponder also is arranged to contain information 30 concerning debiting related to the filling, and that a code read through the sensor from the transponder thereby is matched with data from a sensor unit for identification of the owner or the driver of the vehicle.

35 With owner or driver is meant in the description and the claims, except for the owner or the driver a person who is authorized to fuel the vehicle and thereby cause that an

account or the like is debited.

According to the invention a microwave transponder (0,9 - 25 GHz) mounted close to the filling point of the vehicle has been designed so that it both can be carefully measured with respect to its position, and also that it can be read with respect to its data contents, and possibly also that it can be reprogrammed. A preferred embodiment of the transponder consists in that at certain times it gives away a measurement signal, and at other instants communicates with a data signal. By a thus repeated and time sequential measurement/communication a solution is obtained where the respective signals can be optimized for their purpose.

According to the invention, an active and unique action of the driver of the vehicle is required, alternatively that a biometrical sensing of the driver is made, whereby a higher level system ties together the information from the driver with the information that has been stored/is stored in the transponder. In this way there is no longer any demand to steal the transponder, since a violator with great certainty is not able to repeat the identification of the driver, and he can thereby not make any use of a stolen transponder.

The identification of the driver is in a preferred embodiment made such that the driver keys in a PIN code (Personal Identification Number) in a keyboard close to the side window of the vehicle, but can also make use of so called biometrical methods such as speech/voice recognition, where the driver talks in a code via a microphone close to the vehicle. Other biometrical methods include that the driver enters his finger in a sensing unit for fingerprints close to the vehicle, alternatively that the shape of the palm of the hand is sensed.

In still another embodiment the driver uses a code transmitter or an electronic reflecting data carrier to transfer an identification signal. Alternatively an object belonging to the

driver, such as a card with an optical code, can be used for the identification.

5 All the mentioned methods can be used without the driver having to step out from the vehicle, and thereby give the desired comfort.

10 The methods with biometry, code transmitter, data carrier and optical codes also have the advantage that a code does not have to be memorized.

15 In a preferred embodiment the transponder can partly or completely be written with encrypted data. In this case the advantage of protection against viewing as well as protection against copying between different transponders is obtained, whereby the theft demand for the transponder is furthermore decreased. In addition the risk for unauthorized copying is reduced, e g with transponder data which with a portable reader is caught from a vehicle provided with a transponder on a 20 parking place or the like.

25 Information storage in the transponder is thereby made both in a read memory and in a write/read memory, whereby the read memory is only possible to write once, preferably during manufacturing of the transponder.

30 The read memory is written with a code unique to each transponder, a so called mark, so that each unit is unique and can not be mixed up with others. Permanent writing methods are preferably used, e g in that memory circuits in the data chip of the transponder during manufacture are etched selectively with a laser or are burned by means of coded current pulses in a pattern individual to each transponder.

35 During writing of encrypted data in the transponder the information is encrypted together with the own unique mark of the transponder and possibly a random number, in that the mark

first is read into the unit that makes the encryption. In this way a unique encrypted code is created in the write/read memory of each transponder, even if the information in different transponders, e.g. the code for a certain fuel filling station, should be alike. This makes it much more difficult for unauthorized viewing of the transponder and falsification of it.

10 Another advantage with the encryption technique is that one does not have to distribute transponder lists to the filling stations, but only the system key that has been used for writing of the data carrier with its encrypted data. By aid of the system key the distributed communication units can automatically decide if the data carrier is valid or not, e.g. if a prepaid value stored in the transponder is large enough, if the transponder is valid at the filling place in question etc, without a central system having to be called. In this way communication costs, long response times and vulnerability of the system is avoided. Related debiting does not have to be  
15 made at the same time as the fuelling takes place, but can take place before or afterwards as desired.

20 Nevertheless so called black lists can be distributed at a relatively low cost to the fuel filling stations, since they only contain a minor part of all transponders in the system, and then be locally verified against the unique mark of the transponder.

25 To show that the transponder is used by its right owner, the security may require that a special code, so called PIN code, is used during identification. The PIN code can according to the system described herein be stored in a secure way in encrypted form in the transponder and be compared with the code that is received from the owner at an entering unit localized  
30 close to the fuelling robot. Since the PIN code is encrypted, the security will be sufficient to permit the verification to take place locally and without calling.

A PIN code, however limits the flexibility in the identification since the person has to key it in at each instant. It can then be imagined that a PIN code is keyed in more seldom, e.g. once a month and at the fuelling place that is most often used. The validity period and a code for the special fuelling place is thereby written into the transponder in an encrypted way and can be valid for e.g. a month or a year.

It will furthermore be more secure to store prepaid monetary values in the transponder, that can be debited each time fuelling takes place. The petrol station does then not have to make a call neither to check the PIN code nor to debit a central account, but can function off line. This is especially advantageous in less populated areas and in areas where the infrastructure of society is not well developed as regards handling of electronic payment transactions.

Filling of a new amount into the transponder can take place at the instant of fuelling by the fact that the position sensor also changes transponder data according to an order from a bill counting machine, a bank etc according to the driver's instructions during fuelling, and where a credit card or a so called smart card can be used to authorize the transaction.

The transponder contains in a special embodiment also a write memory that can not be read, and a fast encryption algorithm in hardware and without microprocessor. In the write memory in the transponder one then writes in a transponder key in the form of an encrypted number. The transponder key is created by the fact that, in the unit that makes the writing, the first read unique mark of the transponder is encrypted with a higher level system key.

An advantage with the solution with transponder key and hardware algorithm is that the system can ensure that nobody can imitate the behaviour of the data carrier, that will become different from one communication instant to another. During identification, the communication unit sends a random number to the transponder. The transponder encrypts the random number

with the transponder key according to the encryption alghorithm built in in its hardware, and retransmits the encrypted random number and the mark to the communication unit.

The communication unit can now with the mark, the system key and the random number calculate the transponder key and perform the same encryption as the data carrier to check that the response of the transponder is valid.

11 A special advantage by not using a microprocessor is that the encryption procedure becomes faster, especially since no time is needed to serially feed data between the high frequency junction and the circuits of the microprocessor. Since the serial circuits can operate in synchronism with the high  
15 frequency signals, the communication time is considerably reduced.

20 Another advantage by not having a microprocessor in the transponder is that it can be made much more lean on current, which gives smaller dimensions and lower cost at the same time as both speed and communication range will be good.

25 A portable read/write unit can be used to update the data of the transponder. The portable unit can thereby stay in connection with a central via microwaves within a range of about hundred meters.

30 Data intended for the transponder can comfortably and without wire be gathered from the central to the place where the vehicle is parked, and in the opposite way transponder data can be transferred from the transponder to the central. Since the encryption key thereby does not exist in the portable unit but is in a higher level system, the theft demand for the portable unit will be low. It can not be used in itself to read and  
35 interpret transponder data, but serves as a comfortable communication link for transponder data to and from each place within reach of the communication unit from the central.

The portable unit can also, instead of via microwave

communication, be connected to the central via a cable.

#### Description of the drawings

The invention shall now be described more in detail with reference to embodiments of the invention on the enclosed drawings, where

10 Fig 1 shows a vehicle at an automatic fuel filling station,

Fig 2 shows coding of a transponder,

15 Fig 3 shows schematically encrypted writing and reading of a transponder,

Fig 4 shows the corresponding writing and reading more in detail, and

20 Fig 5 shows communication between transponder and central via a portable communication unit.

#### Description of embodiments

25 Figure 1 shows a vehicle 1 close to an automatic fuelling robot 2. The robot has in the outer end of its movable arm 3 a sensor 4, which is designed to measure the position of a transponder 5, so that with guidance of the transponder it is able to guide its filling tube 6 to the filling place 7 of the vehicle.

30 Close to the vehicle 1 there is a sensor unit 10, which senses the result of a unique action by the driver or biometry, such as the keying in of a PIN code, voice expressions, fingerprints, hand palm pattern etc.

35 The transponder 5 emits continuously, or repeated with certain time intervals, a modulation code 20 shown in fig 2, which comprises a phase and/or amplitude modulated reflex of a microwave signal radiated from the sensor 4, e.g. at 2,45 GHz.

The modulation of the transponder is suitably made without adding new energy to the signal, in that the transponder from the output signal of the sensor 4 creates a modulated signal with information sidebands that are reradiated to the sensor and are there mixed down to base band, e g 32 kHz, for further signal processing.

11 The sensor can also, in a known way, by transmission of a pulse modulated microwave signal to the transponder update its data contents.

15 In a special embodiment pulse modulation can also be used to activate the circuits in the transponder that are causing the side band modulation, while the circuits transfer to a resting state when the pulse modulation disappears. Since the transponder only to a smaller part of its time is in the field from a sensor, the total current consumption will therefore be less than if the modulation takes place continuously.

20 In the embodiment every modulation code from the transponder is divided in a synchronizing/measurement sequence 21 and a data sequence 22.

25 During the synchronizing/measurement sequence 21, phase comparison is made in the sensor so that angular error signals can be created and brought forward for steering of the robot. The measurement will be very accurate since the frequency and the phase of the transponder signal 21 during this time is controlled and unaffected by transponder data and therefore 30 without uncontrolled spectrum widening. The signal is typically controlled from a crystal in the transponder unit, e g by a watch crystal with the frequency 32 768 Hz.

35 During the communication sequence 22 data is transferred from the transponder to the sensor in the form of the signals 22a and 22b. In this case the sequence 21 is used for synchronizing of the decoding circuits in the robot that are to interpret the signal 22a and 22b. The transferred signals 22a and 22b can be coded in a number of different ways, e g according to FSK,

DFSK, PSK or DPSK.

The signals 22a and 22b causes such a spectrum widening in the base band signal (e g around 32 kHz) that the precision of the measurement during the time 22 will be considerably reduced. This is, however, not a problem, since the measuring sequence 21 is repeated often enough so that the robot can not move very far between each measuring instant. A typical intermediate time between two measurement sequences can e g be 100 ms, while the measuring sequence in itself can be in the order of 10 ms.

When the robot has now measured the position of the transponder and has docked with the filling point of the vehicle, a verification is needed that the identity of the driver is fitting with data from the transponder.

This takes place in the shown example in that the driver keys in a PIN code in the terminal 8 placed close to the side window. The higher level system has before that received information about which account that is to be debited, and which PIN code that is connected with the account can alternatively be gathered from a central that is called. Matching of the transponder code with the keyed in code leads to the fact that the robot can start its fuelling pump and complete the fuelling. The matching takes place by means of circuits including a microprocessor or computer belonging to the robot.

In another embodiment voice entering is used, whereby a microphone 11 is applied at the sensor unit 10, to which a voice recognition system is connected. The interpretation of this system of the pronounced code of the driver, e g a PIN code in the form of a number of talked figures, is then matched with the transponder code.

Still another embodiment is using identification with an optical sensor close to the vehicle that recognizes an object brought by the driver such as a card with a barcode or a dotcode.

The sensor unit can also be designed to receive signals from a code transmitter or an electronic data carrier that preferably operates in the visual, IR, radio or microwave range, alternatively operates with ultrasonic technology.

5

In the transponder mounted on the vehicle also other information can be stored, such as about discounts, fuel quality etc, which is especially advantageous if the filling station is remotely located and a non called system therefore 10 is used for the debiting.

In the same way it is of advantage if a prepaid value has been stored in the field of the transponder field 22b, which value is read by the sensor unit 4, is modified according to the cost 15 for the performed filling and is rewritten in the data field 22b of the transponder.

The above mentioned method to encrypt the transponder information can thereby be used, and then the transponder 20 unique code field 22a is used as a so called mark, while the code field 22b is used for data and possible random information.

The PIN code and/or a balance related to the payment is then 25 preferably pre programmed in the data field 22b of the transponder, whereby the data field of the transponder is encrypted with information from a transponder unique and not changeable code in the transponder 22a, an encryption key and possibly a random number. This technology is more accurately 30 described in connection to figures 3 and 4, where the mark 22a corresponds to the field 47 and where the encrypted part of the data field 22b corresponds to the field 51.

Information to the driver is given on a display unit 9, e.g. 35 instructions for the debiting and information about remaining amount in the transponder in case it is preprogrammed with money related information. The display unit can also be used in conjunction with the transponder being filled with a money related value via a bill reader, credit card, smart card or

other technology.

The sensor unit 10 can thus include a keypad, microphone, video camera and image processing circuits, fingerprint detector, hand palm sensor, magnetic card reader, so called smart card reader, communication unit for code transmitter and data carrier etc.

10 Figures 3 and 4 show writing and reading of an encrypted transponder according to the invention, although the embodiment with hardware algorithm in the transponder is not shown in figure.

15 In figure 3 two communication units 41, 42 and a transponder 43 are shown, where the first communication unit is used for encrypted writing of data into the transponder and the other is used for reading. The transponder thus brings encrypted information from one place to another and thereby constitutes a media.

20 The transponder is designed to be communicated with microwaves 44, 45, so that during writing it is illuminated with a coded microwave signal 45, alternatively during reading emits a reflex 44 where data, without new energy having been added to the microwave signal, is modulated onto an illumination signal 45 emitted from the communication unit, which during the modulation time is essentially continuous. The communication unit 41 can be a sensor 4 at a fuelling station with bill reader and/or credit card/smart card reader, and the communication unit 42 can be a sensor at a filling station which only is intended for filling of fuelling and not for filling money related amounts to the transponder.

35 The memory of the data carrier, i e the memory of the transponder, comprises both a read only part 47 with a code unique for the data carrier, the so called mark, and a read and write part 48, a so called write/read memory, where variable data can be written. In the communication units 41, 42 there is also one and the same encryption key 49.

Figure 4 shows an embodiment where at least a part 51 of the read/write memory 48 is readable from outside, and where the same data can be stored in different transponders despite that the bit pattern in the memory part 51 through said encryption is different from data carrier to data carrier. Encryption according to what is later mentioned about hardware key in the transponder can, but does not have to, be included in the transponder since all applications do not require this function.

10

The first communication unit 41 is first reading the unique mark 47 and then encrypts the mark and the basic information 56 in the write/read memory 51.

15

When the same system key 49 is used in the second communication unit 42, user data 56 can be recovered 55 in that the mark 47 then read from the transponder and the system key 49 are used for decryption of the encrypted information 52 that has been stored in the write/read memory 51 of the data carrier.

20

In addition to what has been described so far, one can, in addition to mark 47 and system key 49 also make use of a random number 53 created in the first communication unit 41 during encryption of the information 52 to the memory part 51 of the transponder. In this case the recovered user data 55 are separated from the recovered random number after decryption. Normally the random number 54 is thrown away after recovery.

30

Encrypted information in the memory 51 of the transponder can thus concern validity classed information intended to be varied only at certain communication instants, and then represents e.g. validity time, a PIN code, a geographical area or an authority class. It can also concern value related information intended to be varied at each communication instant, such as monetary value to be used for fuelling.

35

The algorithm for writing of data in the transponder is normally of a symmetrical type, while an asymmetrical algorithm can be used for transferring of the system key in itself,

40

possible PIN code, debiting data etc over the ordinary telecommunication network.

5 This transfer then takes place between different communication units, alternatively between a called central and a communication unit.

10 Figure 5 shows a portable communication unit 30, which via microwaves at a relatively short distance can write and read information in the transponder 5 and at relatively large distance also can communicate this information with a central 31. Because the communication unit is designed fully transparent for data, it is obtained that the encryption key does not have to be in the portable unit whereby the theft 15 demand for it is reduced.

The communication unit can also be connected to the central via a serial line 32 instead of, or as a complement to, the earlier described microwave connection.

## CLAIMS

1. System for debiting at automatic fuelling of vehicles, where a microwave transponder (5) close to the filling point of the vehicle is used for positioning of a fuelling robot (2) by position measurement with a sensor (4) in the movable arm (3) of the robot, characterized in that the transponder also is intended to contain information concerning the debiting related to the filling, and that a code (22) read via the sensor from the transponder thereby is matched with data from a registration unit (10) for identification of the owner or driver of the vehicle.

10

2. System according to claim 1, characterized in that said identification is made by recognition of a driver unique action such as entering of a PIN code and/or in that the biometrical properties of the driver are sensed and/or in that information from an object brought with the driver is sensed.

15

3. System according to claim 1 or 2, characterized in that the input means of the sensor unit comprises a keypad (8) for entering of PIN code, a voice and/or speech recognition equipment with microphone (11), a fingerprint detector or a hand palm sensor.

20

4. System according to claim 1 or 2, characterized in that an optical sensor close to the vehicle recognizes an object brought with the driver such as a card with barcode or dot code upon it.

25

5. System according to any of the previous claims, characterized by that a sensor close to the vehicle interprets signals from a code transmitter or electronic data carrier brought by the driver, where the brought unit operates in the visual, IR, radio or microwave area, alternatively functions with ultrasonic technique.

30

6. System according to any of the previous claims, characterized by that the transponder, with or without time intervals, emits a synchronising/measuring sequence (21) with

40

controlled frequency and phase for measurement of the position of the transponder, and also emits a communication sequence (22) in which information about an account related to the debiting has been stored.

7. System according to any of the previous claims, characterized in that the PIN code and/or an account related to the payment or balance are stored in a write/read memory (48) in the data field 22b of the transponder, and that the whole or part of the transponder data field (51) is encrypted with information from a unique and not changeable code in the transponder (22a; 47), an encryption key (49) and possibly a random number (53).

15 8. System according to any of the previous claims, characterized in that the data field (48) of the transponder before the filling of fuel contains information about a prepaid amount, that after the fuel filling is modified by rewriting of a correspondingly changed amount in the data field.

25 9. System according to any of the previous claims, characterized in that the transponder is designed to receive a random number and from this and a memory possible to write but not readable in the transponder according to a hardware algorithm in the transponder calculate a number (transponder key), emit this and its mark, and where the system reads the emitted information and by a control calculation confirms the information of the transponder despite that its emitted information varies from 30 one instant to another since the random number varies.

35 10. System according to any of the previous claims, characterized by that it also includes a portable communication unit (30), that via microwaves can write and read information in the transponder (5), and where the portable unit via microwaves or cable also can communicate the transponder information with a central (31).

40 11. System according to any of the previous claims,

characterized by that the communication unit (30) can transfer encrypted information between the transponder and the central without that any encryption key exists in the communication unit.

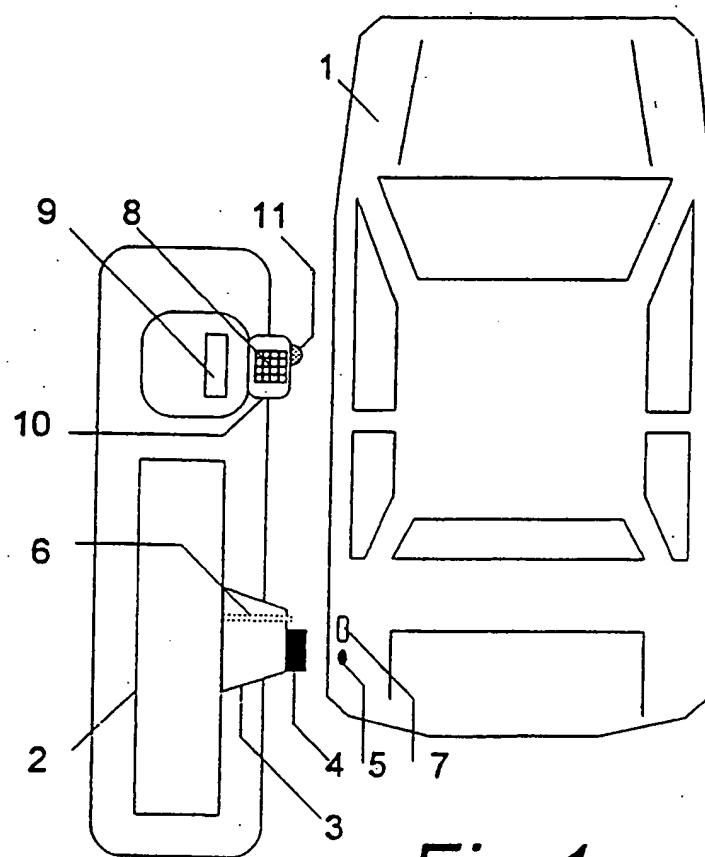


Fig 1

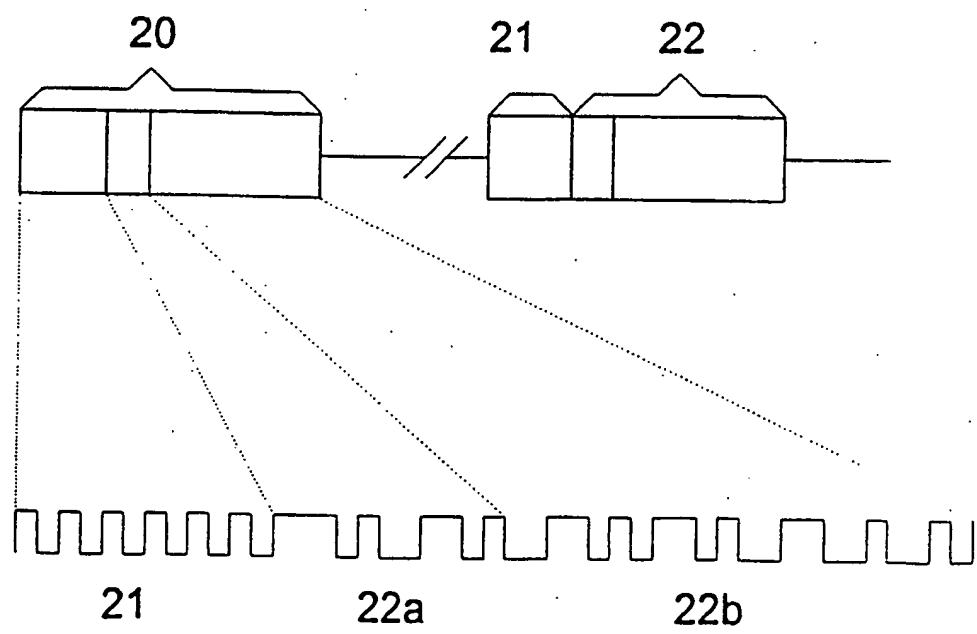


Fig 2

2/3

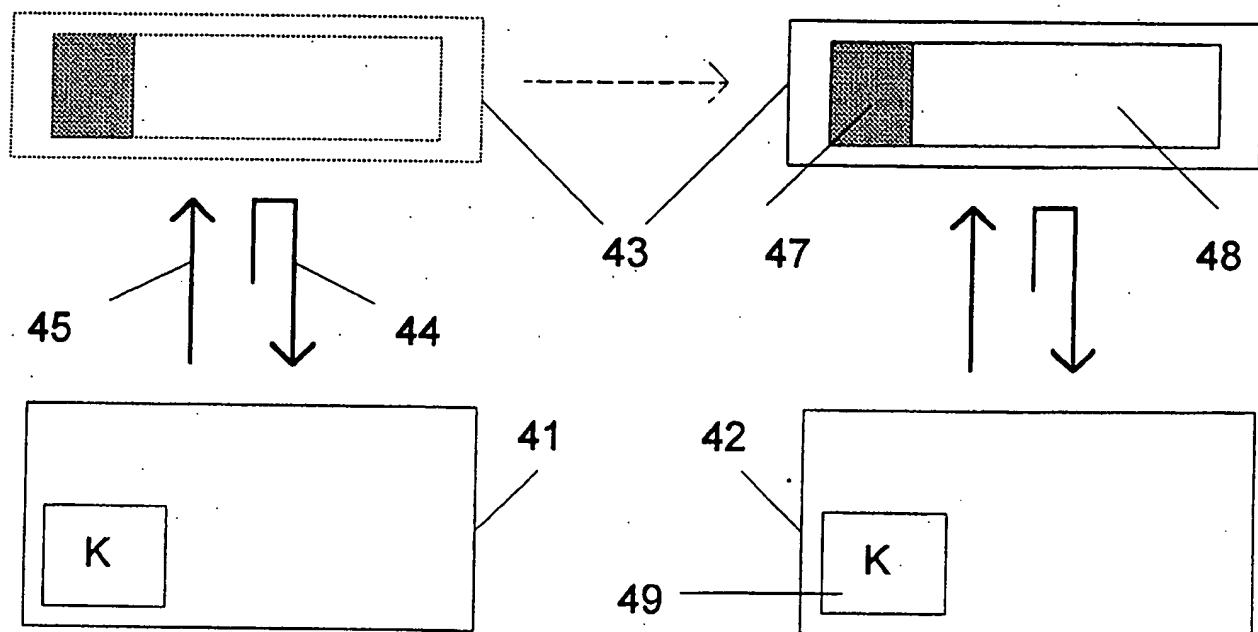


Fig 3

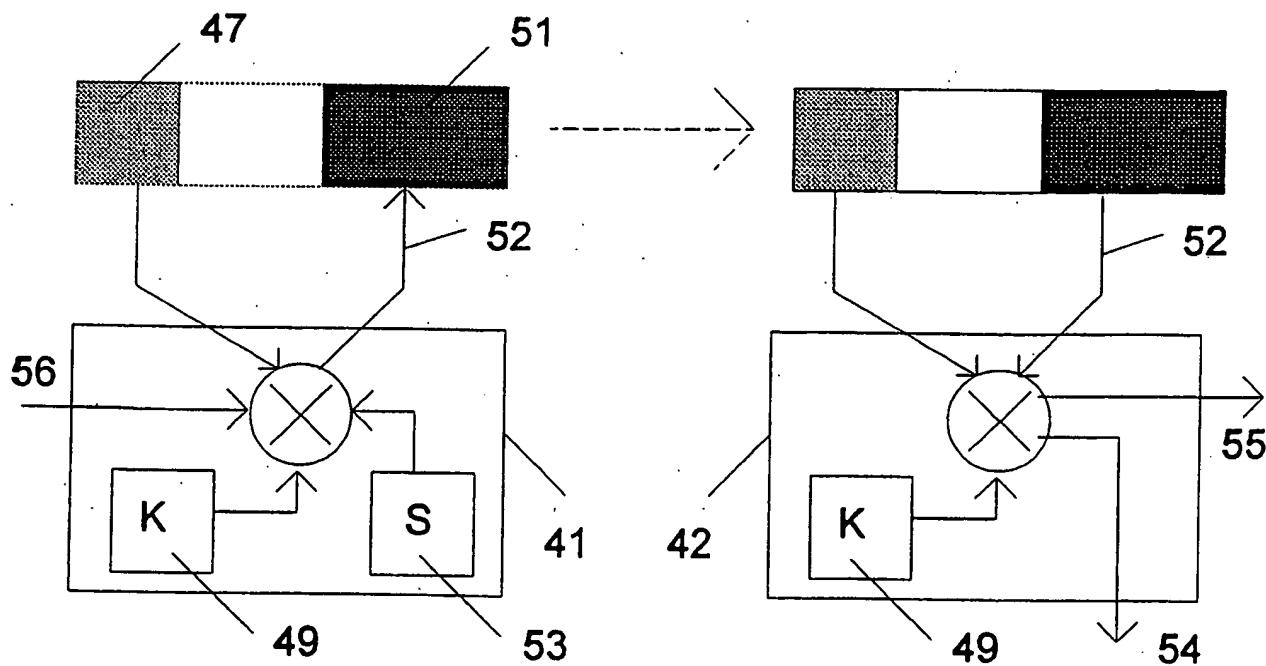
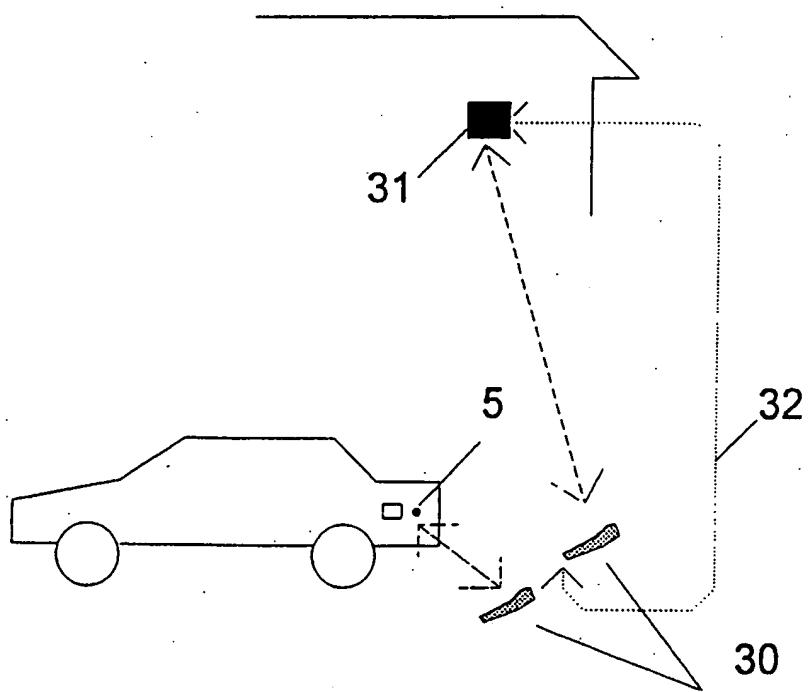


Fig 4

SUBSTITUTE SHEET



*Fig 5*

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 94/00508

## A. CLASSIFICATION OF SUBJECT MATTER

IPC6: B67D 5/08

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: B67D, B60S

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE, DK, FI, NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## WPI, CLAIMS

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E, X	SE, A, 9303879-2 (STAFFAN GUNNARSSON), 30 May 1994 (30.05.94), the whole document --	1-11
X	SE, A, 9203590-6 (STAFFAN GUNNARSSON), 23 July 1993 (23.07.93), the whole document --	1-11
X	WO, A1, 9315418 (SAAB-SCANIA COMBITECH AKTIEBOLAG), 5 August 1993 (05.08.93), page 18, line 15 - line 23; page 19, line 12 - line 17, figure 7, claims 13-18 --	1-11
A	US, A, 4303904 (NORMAN E. CHASEK), 1 December 1981 (01.12.81), abstract --	1-11

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	
"A"	document defining the general state of the art which is not considered to be of particular relevance
"E"	earlier document but published on or after the international filing date
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O"	document referring to an oral disclosure, use, exhibition or other means
"P"	document published prior to the international filing date but later than the priority date claimed
"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X"	document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y"	document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&"	document member of the same patent family

Date of the actual completion of the international search

3 January 1995

Date of mailing of the international search report

10-01-1995

Name and mailing address of the ISA/  
Swedish Patent Office  
Box 5055, S-102 42 STOCKHOLM  
Facsimile No. +46 8 666 02 86Authorized officer:  
Mårten Hulthén  
Telephone No. +46 8 782 25 00

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 94/00508

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP, A2, 0418744 (ETS ELEKTRONIK GMBH), 27 March 1991 (27.03.91), page 11, line 14 - line 39, figures 1,4,11, claims 9-11 --	1-11
A	EP, A1, 0476858 (RYAN, MICHAEL C.), 25 March 1992 (25.03.92), figure 1, claim 21 --	1-11
A	WO, A1, 9406031 (CORFITSEN, STEN), 17 March 1994 (17.03.94), figures 1,2, abstract -- -----	1-11

## INTERNATIONAL SEARCH REPORT

Information on patent family members

26/11/94

International application No.

PCT/SE 94/00508

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
SE-A- 9303879-2	30/05/94	NONE		
SE-A- 9203590-6	23/07/93	NONE		
WO-A1- 9315418	05/08/93	AU-A-	3413393	01/09/93
		EP-A-	0623219	09/11/94
		NO-A-	933564	08/11/93
		SE-A-	9200209	06/01/93
		SE-A-	9203590	24/07/93
		AU-A-	3465293	01/09/93
		EP-A-	0616730	28/09/94
		JP-T-	6502281	10/03/94
		SE-A-	9200210	06/01/93
		WO-A-	9315417	05/08/93
		WO-A-	9323833	25/11/93
		WO-A-	9325918	23/12/93
		SE-A,D-	9303879	31/05/94
US-A- 4303904	01/12/81	NONE		
EP-A2- 0418744	27/03/91	DE-A-	3930981	28/03/91
EP-A1- 0476858	25/03/92	AU-B-	643063	04/11/93
		AU-A-	8278991	05/03/92
		CA-A-	2049874	28/02/92
		US-A-	5204819	20/04/93
WO-A1- 9406031	17/03/94	NONE		

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

### **IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**